オープンソースの「今」を伝える
オープンソースカンファレンス
2014 Fukuoka

JPCERT CC®

Lessons (to be) Learned from Handling OpenSSL Vulnerabilities

2014年11月22日

JPCERTコーディネーションセンター
情報流通対策グループ
脆弱性解析チームリーダー
久保 正樹

2014年に JPCERT/CC がハンドリングした OpenSSL の脆弱性 を振り返る

OpenSSL とは

- 暗号化の機能(SSL/TLS/DTLS)を提供するライブラリ
- オープンソース
- Apache License 1.0
- LibreSSL (OpenBSD) と boringssl (Google) に最近フォーク
- 多くのサーバで利用されている
- 一部のクライアントでも使用されている
  - Android (SSLSocketFactory等), Chrome for Android 等

SSL/TLS 関連の脆弱性 (2014)

OpenSSL 関連

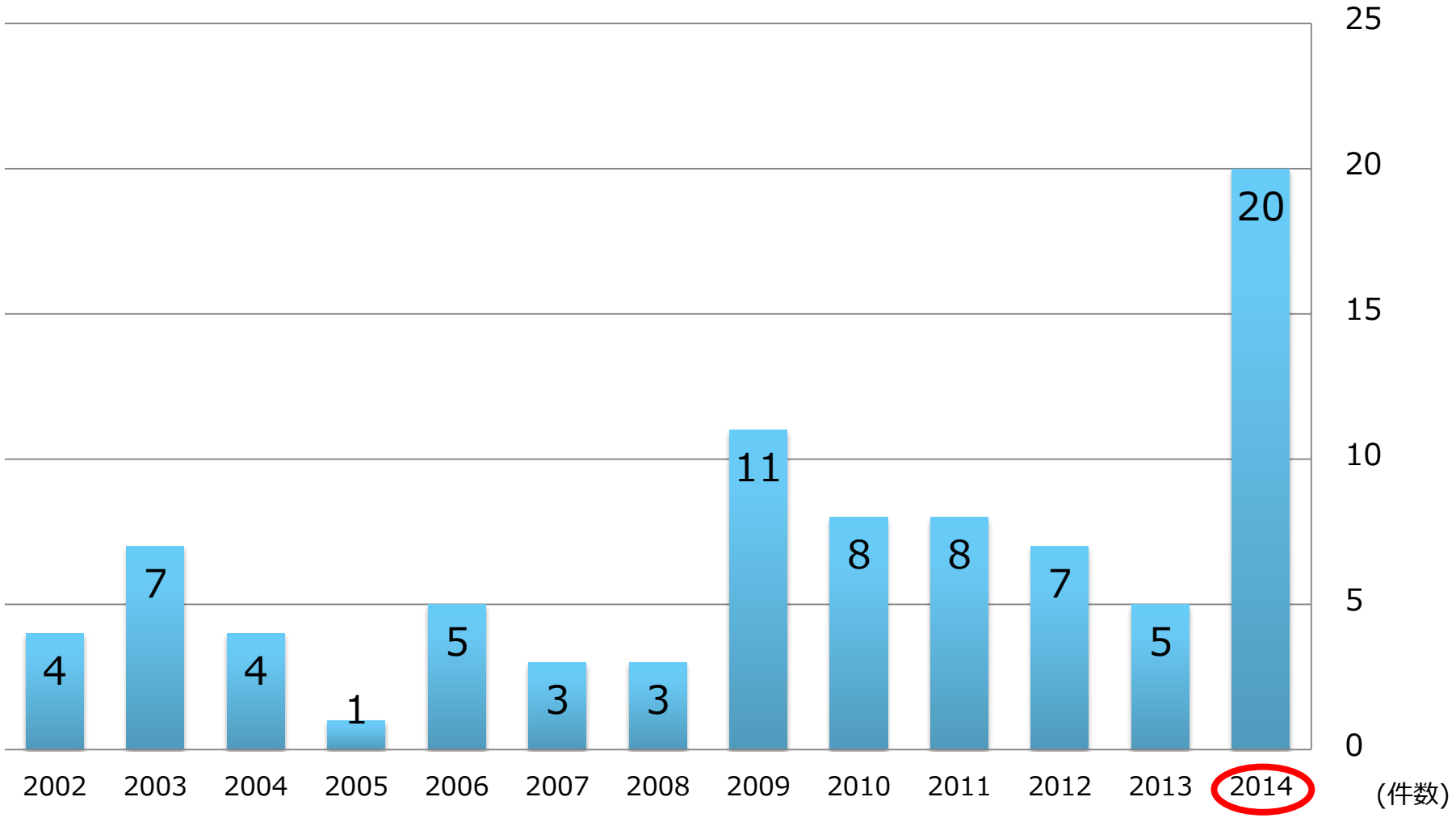
4月8日	JVNVU#94401838	OpenSSL の heartbeat 拡張に情報漏えいの脆弱性
6月6日	JVN#61247051	OpenSSL における Change Cipher Spec メッセージの処理に脆弱性
8月11日	JVNVU#93614707	OpenSSL クライアントにナルポインタ参照の脆弱性
10月16日	JVNVU#98283300	SSLv3 プロトコルに暗号化データを解読される脆弱性(POODLE 攻撃)

SSL/TLS 関連の脆弱性 (2014)

- サーバ証明書を**検証しない**問題
  - JVNで11件公表
  - Androidアプリに多数見つかる
    - SslError 回避のバッドノウハウ流布が原因？
  - USでは、連邦取引委員会(FTC)が問題視して2社を指導

- 関西オープンソース2014で JPCERT/CC 戸田が講演
  - ～誰かの失敗を他山の石に～脆弱性事例に学ぶセキュアコーディング「SSL/TLS証明書検証編」
  - https://k-of.jp/2014/session/563

OpenSSLの脆弱性



[source] https://www.openssl.org/news/vulnerabilities.htm

情報セキュリティ早期警戒パートナーシップ

発見者

IPA
(受付)

CERT/CC
NCSC-FI
(調整)

JPCERT/CC
(調整)

開発者の皆さん

個人

企業

オープンソース
コミュニティ

JVN
(公表)

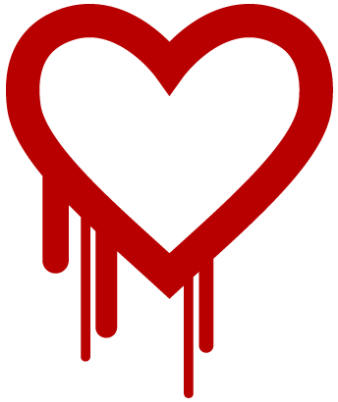
エンドユーザ

企業ユーザ

マスメディア

SIer

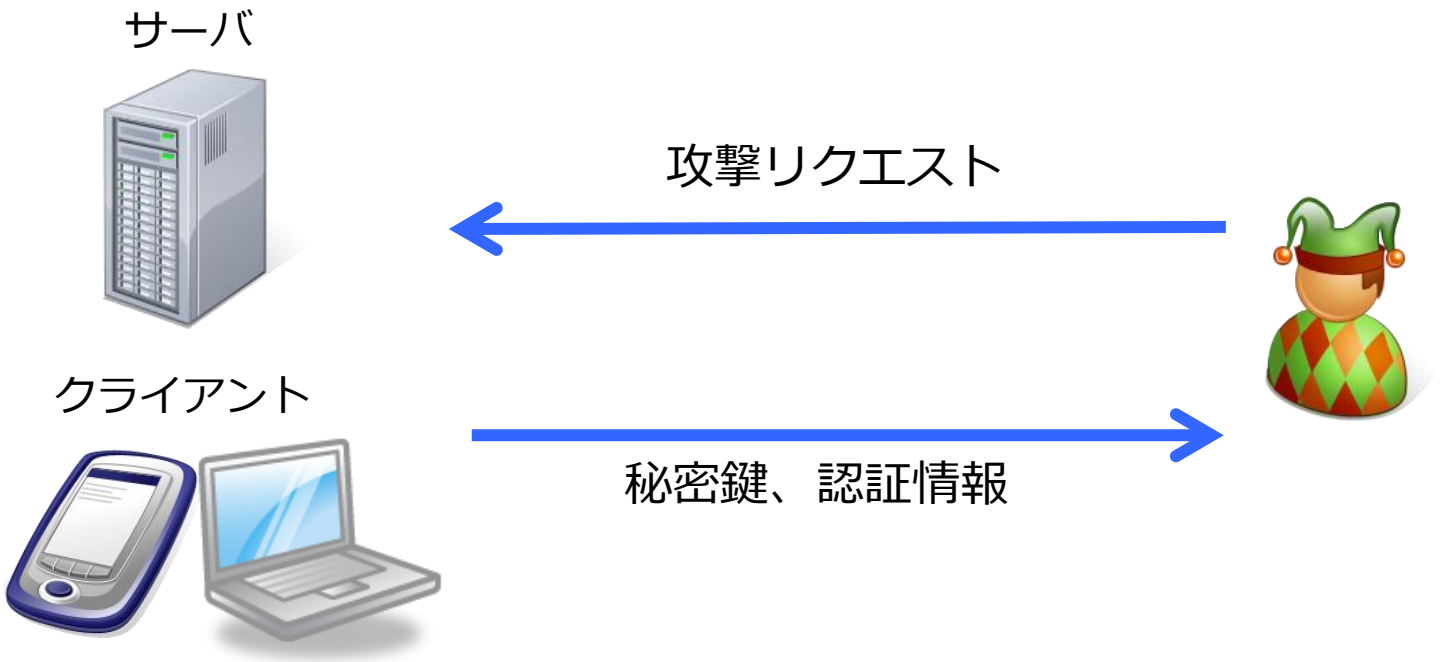
などなど



The Heartbleed Bug

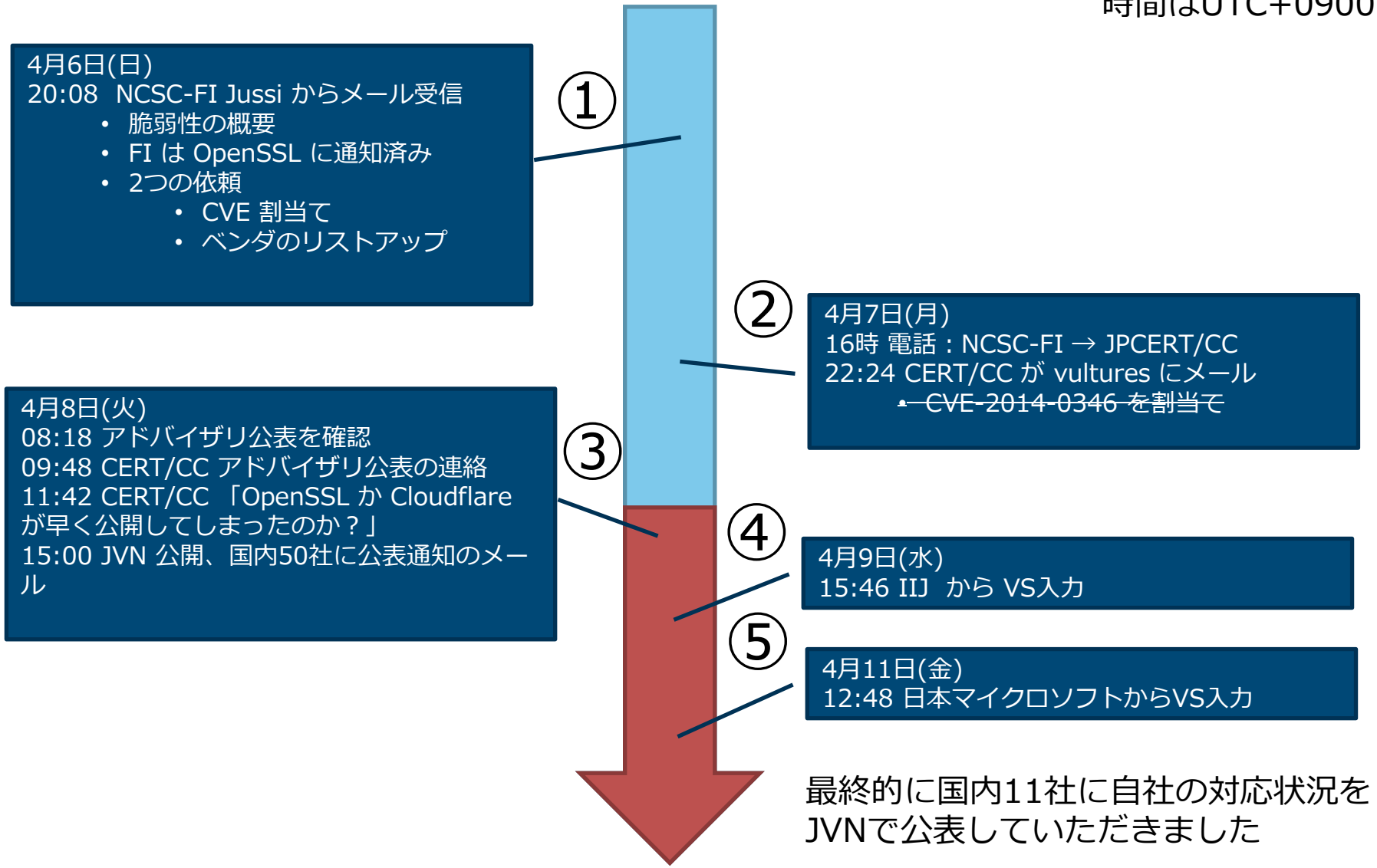
Heartbleed 脆弱性とは

- プロセスメモリ上のTLS 秘密鍵が漏洩する問題
- OpenSSL 1.0.1 が影響を受ける
- Codenomicon の研究者が脆弱性を発見
  - のちに Google も同時に問題を発見していたことが判明

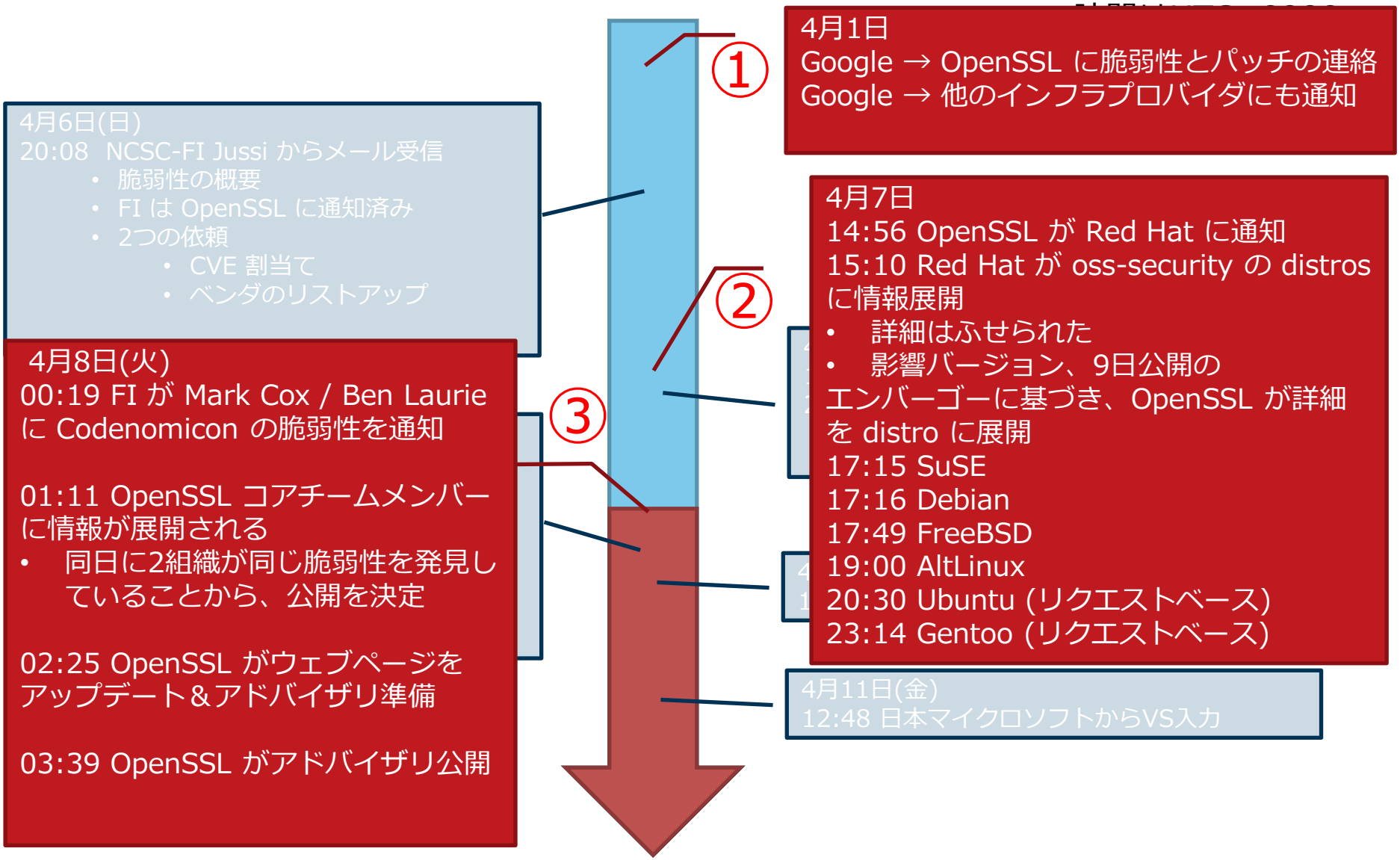


時系列 (JPCERT/CC)

時間はUTC+0900



時系列 (OpenSSL)



脆弱性公表について

- OpenSSLが直接連絡したのは Linux Distro 5社だけ
  - —Red Hat, SuSE, Debian, FreeBSD, AltLinux
  - —残りの distro は oss-security 経由
- Akamai, Cloudflare, Facebookには事前にパッチが提供されていた
  - —Google 経由で連絡が行っていたと推測される
- 詳しい経緯
  - —The Sydney Morning Herald – *Heartbleed disclosure timeline: who knew what and when*

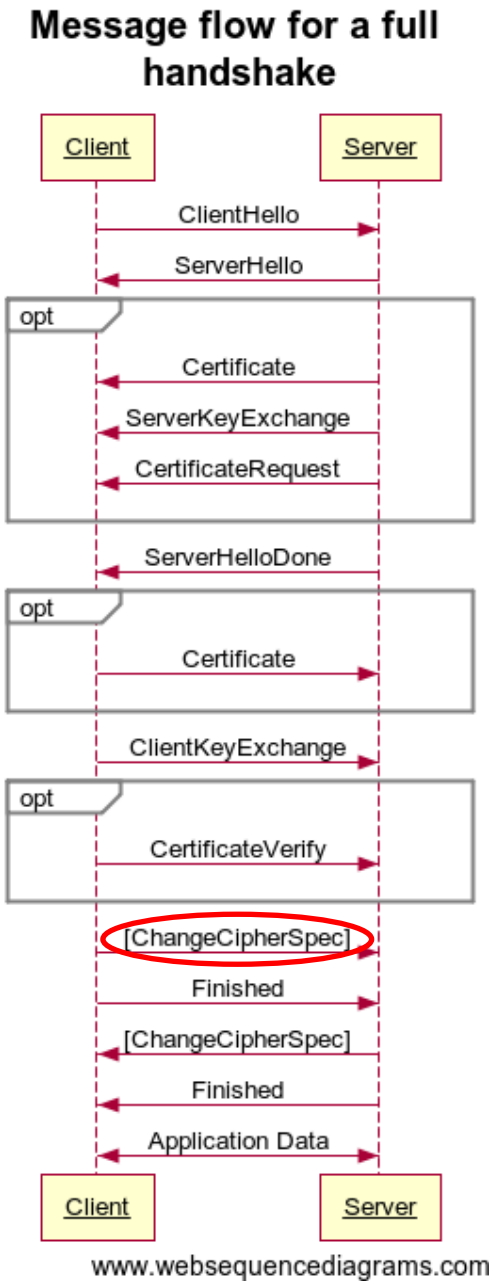
Lessons Learned

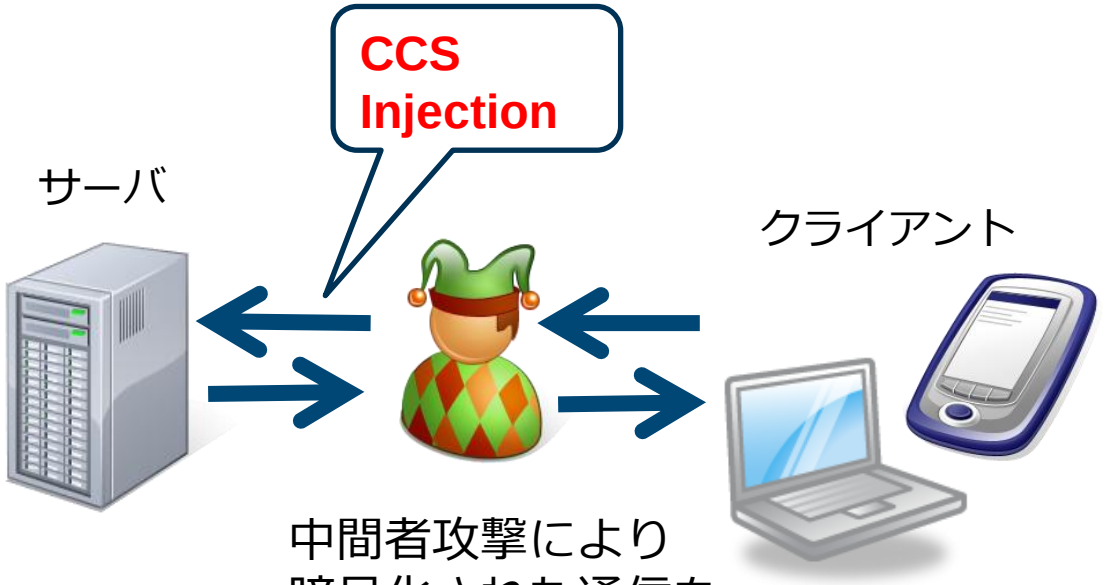
- 調整機関 (JPCERT/CC, CERT/CC, NCSI-FI) は調整相手しか見えなかった
- OpenSSL 自身も限られた情報に基づきハンドリング
  ―前倒し公表は適切であったといえる

CCS Injection Vulnerability

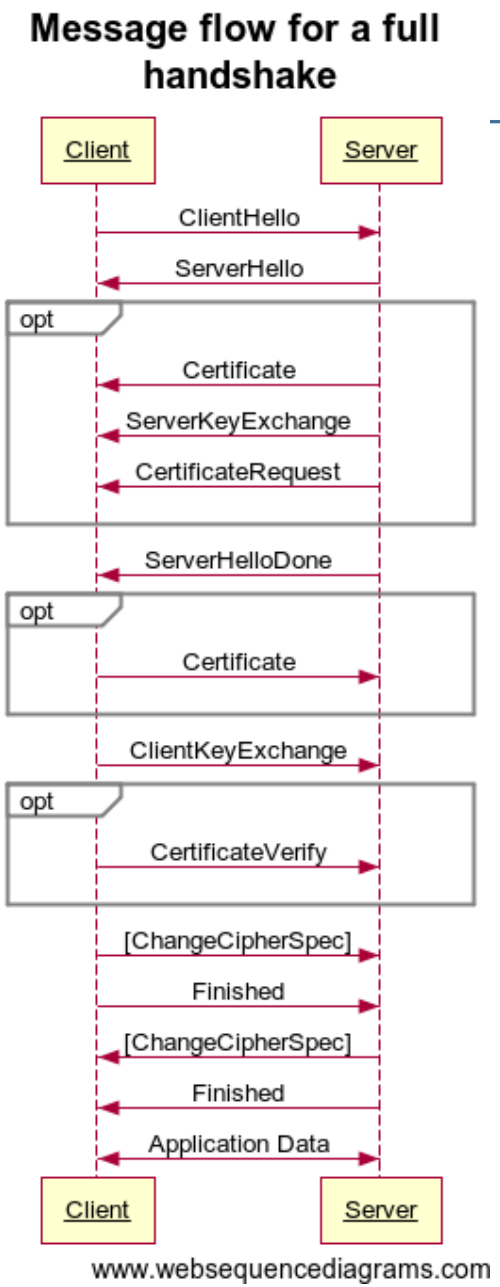
CCS Injection 脆弱性とは

- サーバとクライアントが暗号化通信を開始する手順(ハンドシェイク)の途中で、不正な信号（**change_cipher_spec**）を受け取ると、通信に使われる暗号鍵が予測可能なものになる
  - —通信内容の解読、なりすましに悪用される
- 中間者攻撃が必要
- レピダムの菊池さんが発見者
  - —『OpenSSLのバグを見つけた話』
    IIJイノベーションインスティテュート
    IIJlabセミナー
    http://www.iij-ii.co.jp/lab/seminars/

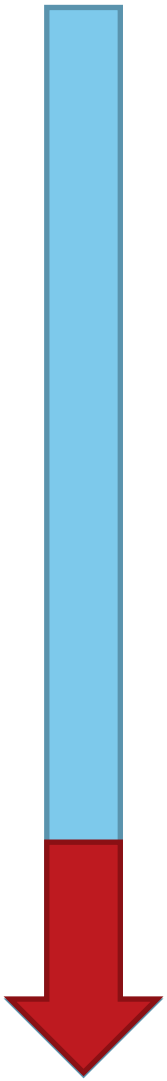




SSL/TLS のハンドシェイク

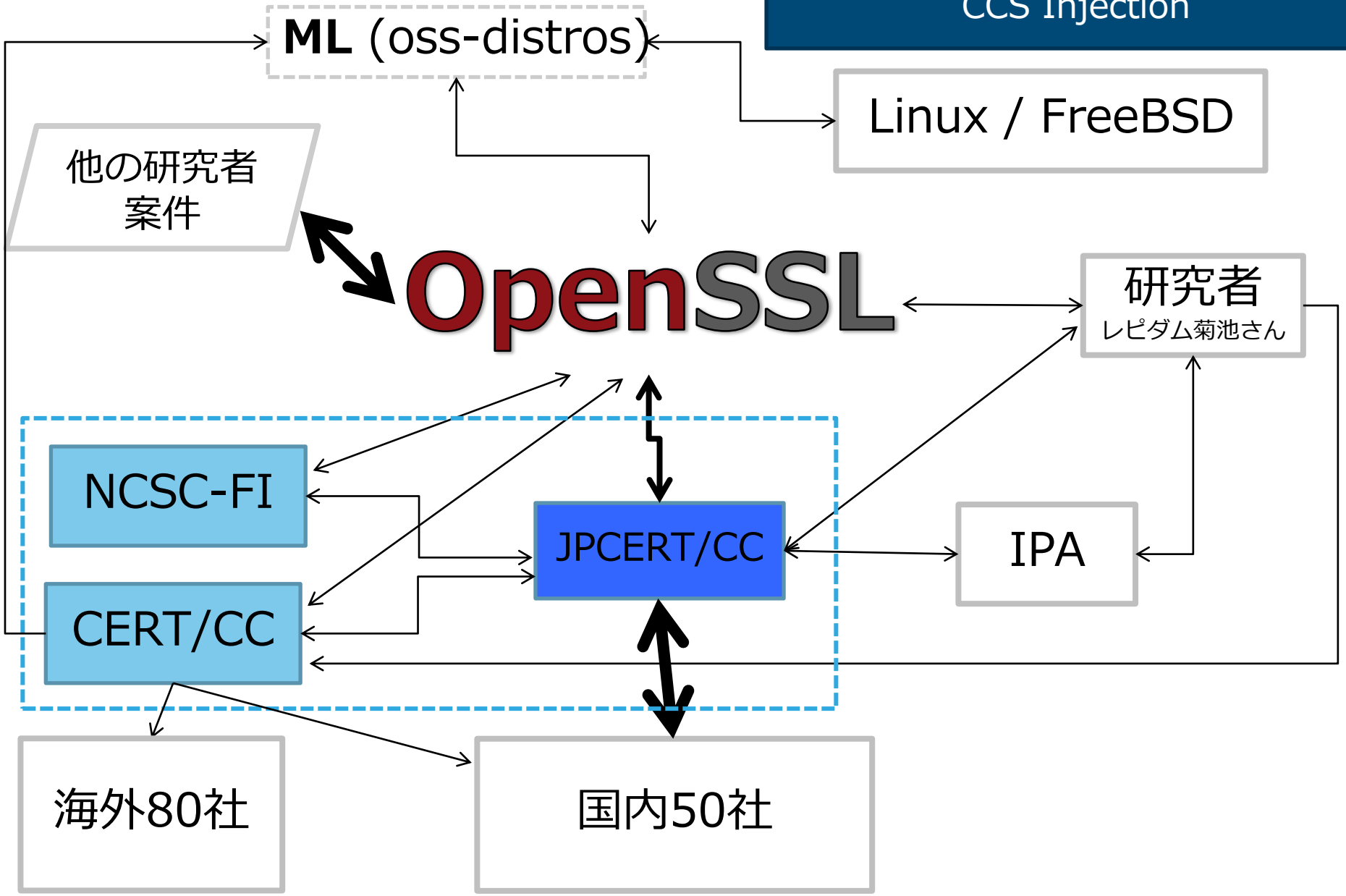


時系列 (JPCERT/CC)



4月23日(水)	IPAから届け出の連絡
4月24日(木)	発見者から追加情報1
4月25日(金)	発見者から追加情報2 検証 & 詳細情報翻訳開始
5月1日(木)	OpenSSL に詳細送付
5月8日(木)	発見者から追加情報3
5月9日(金)	発見者からCERT/CCにも連絡したとのこと
5月12日(月)	発見者から追加情報4(パッチ) CERT/CC に連絡
5月14日(水)	NCSC-FI に連絡 国内約50社に概要通知
5月15日(木)	6月上旬公開を50社に通知
6月5日(木)	OpenSSL、NCSC-FI アドバイザリ公開
6月6日(金)	JVN公開（30 wdays / 44 days）

ハンドリングの実態
CCS Injection



ハンドリング中に頂いた質問1

弊社の製品も対策が必要だが、
OpenSSL からパッチやアドバイザリーは
まだ出ていなません。

弊社側でOpenSSLのサイトを見続ける必要があるのでしょうか。

それとも JPCERT/CC からのアナウンスを待つことになるでしょうか。

回答1

OpenSSL のアドバイザリを最短・確実に入手する方法

1. OpenSSL のアドバイザリを地道にウォッチ
2. JPCERT/CC からの JVN 公開通知を待つ
3. oss-security ML を購読
   - OpenSSL アドバイザリ公開とほぼ同時にメールが流れる
   - 技術ネタのトラフィックがそれなりにあるので、見落とさないように気をつけないとダメ

JVN では、JPCERT/CC や CERT/CC が調整していない案件でも、脅威度の高いと判断される脆弱性についてはアドバイザリを公開します

- ex. POODLE

ハンドリング中に頂いた質問2

早期警戒パートナーシップガイドライン P.10

また、JPCERT/CC は、**OSS に関する事前通知を、開発者コミュニティに加えて、必要に応じて以下へ通知します。**
・OSS を導入した製品の開発者
・ディストリビュータ・製品の仕様を決定するサービス提供者（例：携帯電話会社）

これは、開発者コミュニティによる脆弱性対応が困難でかつ発表もされない場合に、当該 OSS を導入した製品の開発者やディストリビュータ、製品の仕様を決定するサービス提供者は、その事実を知りうる手段がないが、社会的影響を考慮するとそれらの脆弱性対応が重要であるケースが想定されるためです。

今回のOpenSSLは6月にパッチがリリースされるので上記には該当しないと理解。

情報公開前に脆弱性情報を通知した意図は何でしょう？（**普段のフローとは違って見えた**）

回答2

- OSS 脆弱性の事前通知は、BIND や Apache Tomcat の脆弱性でもこれまでやってます
  - 脆弱性の詳細や検証コードまでそろった形で情報提供した点が普段と違って見えたのかも

- これまで「せめて公開日は知りたい」「パッチの事前提供を受けたい」などの要望がある中での情報提供

Lessons (to be) Learned

JPCERT/CC ⇄ 開発者 (1/2)

- 事前情報提供は、開発者の皆さんの役にほんとうに立ったのだろうか？
  - 今回は運良く、レピダム菊池さん提供の精度の高い検証データがあった
  - OpenSSL からパッチの事前提供はなし
  - あくまでOpenSSL が修正した6件の脆弱性のうちの1つ

- 「メディアでも話題になる重要案件は社内調整もあり役に立ちます」という声も

JPCERT/CC ⇄ 開発者 (1/2)

- フィードバックはとてもありがたいです
  - 検証結果を共有して下さった IIJ、ヤマハ、横河電機
  - 特に IIJ さんの影響範囲に関する分析は、アドバイザリ作成時に参考にさせて頂きました

JPCERT/CC ⇄ OpenSSL

- **ミドルマン**にならないために
  - —発見者から、IPA・JPCERT/CC、CERT/CC、OpenSSLの3者に連絡が行ってしまった
  - —OpenSSL に x 3++ のやり取りが発生
    - 余計な負担がフラストレーションを招く結果に

JPCERT/CC ⇄ CERT/CC|NCSC-FI

- 国際連携の認知度向上キャンペーン
  - ― 連携していることが知られていない
  - ―調整機関 ML (vultures)
  - ―開発者、研究者に対し国際連携の理解を広める活動

- Next vultures F2F meeting
  - ―2015年春@RSA Conference
  - ―US の Vendor ミーティングと共催

脆弱性発見者・研究者の皆さんに知っておいてほしいこと

- まずは JPCERT/CC, IPA にご連絡を
  - —開発者との調整活動を行っているCERT組織は世界で3つ
    - JPCERT/CC, CERT/CC, NCSC-FI
  - —NDAを結んで連携しています
- JPCERT/CC は CVE の採番機関です
- 海外の開発者とも普段からやりとりしています
  - —Adobe, Apple, Google, Android, OpenSSL etc…
- JPCERT/CC は Responsible Disclosure の精神にのっとって調整します

OSS開発者の皆さんに知っておいてほしいこと

- 2つのポリシーがあるとスムーズです

- 脆弱性取扱いポリシー
  - 脆弱性の届け出先アドレス
  - 対応の流れ
  - 脆弱性公表ページ
  - セキュリティ問題に「前向き」な姿勢

- 脆弱性公表ポリシー
  - ユーザがリスクを判断できる情報の公表
  - 脆弱性のリスクを低減する方法の提示（パッチ、ワークアラウンド）
  - 発見者・研究者に対する acknowledge

OpenSSL の
セキュリティポリシー

OpenSSL Security Policy

- 2014年9月7日に第1版が公開された
  - —https://www.openssl.org/about/secpolicy.html
- 脆弱性を3段階の脅威に分類してハンドリング
  - —低：開発中のブランチで即修正。必要に応じてバックポート
  - —中：次のセキュリティfixでまとめて修正
  - —高：なる早でバージョンアップ対応（サポート中のバージョンのみ）
- 事前通知は、基本的に OS distro に対してのみ
  - —調整機関に事前通知やパッチ提供は行わない

(参考) ISC Vulnerability Disclosure Policy

- ISC の Vulnerability Disclosure Policy が 10/31付けで更新された
- Before
  - JPCERT/CCはメーリングリスト経由で事前提供を得ていた
- After
  - サポート顧客、DNS オペレータ、OS ディストリビュータのみが事前提供を受けることとなった
- JPCERT/CC は、公開当日に ISC から公開の連絡を受け、各方面 (国内開発者、APCERT、PacCERT、AfricaCERT) への展開を行う予定
- 詳細：https://kb.isc.org/article/AA-00861/0

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：office@jpcert.or.jp
- Tel：03-3518-4600
- Web: https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- Web: https://www.jpcert.or.jp/form/

ご清聴ありがとうございました。

参考資料

OpenSSL Security Policy Last modified 7th September 2014 全訳

はじめに (Introduction)

Recent flaws have captured the attention of the media and highlighted how much of the internet infrastructure is based on OpenSSL. We've never published our policy on how we internally handle security issues; that process being based on experience and has evolved over the years.

昨今の(OpenSSLの)欠陥はメディアの注目を集め、いかに多くのインターネット基盤がOpenSSLに依存しているかを浮き彫りにした。我々(OpeSSL)はこれまで、内部でどのようにセキュリティ問題を取り扱うかのポリシーを公開したことはない。ハンドリングプロセスは、経験に基づくものであり、年月を経て発展してきた。

セキュリティ問題の報告について (Reporting security issues)

We have an email address which can be used to notify us of possible security vulnerabilities. A subset of OpenSSL team members receive this mail, and messages can be sent using PGP encryption. Full details are at https://www.openssl.org/news/vulnerabilities.html

問題の可能性があるセキュリティ脆弱性を我々に通知するためのメールアドレスを我々は設けている。OpenSSL開発チームの一部のメンバーがこのメールを受信する。メッセージはPGPで暗号化してもよい(訳注1)。詳細はこのページを参照してほしい https://www.openssl.org/news/vulnerabilities.html

When we are notified about an issue we engage resources within the OpenSSL team to investigate and prioritise it. We may also utilise resources from the employers of our team members, as well as others we have worked with before.

問題の通知を受け取ると、OpenSSL 開発チームの中でリソースを確保し、問題の調査と優先度付けを行う。場合によっては、メンバーの雇用主のリソースを借りたり、過去の協力者の力を借りることもある。

(訳注1) openssl-security@openssl.org の鍵 (key ID:89A36572)は今や誰も復号できないらしく、この鍵で暗号化すると怒られます。OpenSSL Core and Development Team 開発者個人のPGP鍵を使いましょう。

背景事情 (Background) 1/2

Everyone would like to get advance notice of security issues in OpenSSL. This is a complex topic and we need to set out some background with our findings:

誰しも OpenSSL のセキュリティ問題の事前通知を受けたいだろう。これは一筋縄ではいかない話題であり、我々が発見した背景事情を示す必要がある。

The more people you tell in advance the higher the likelihood that a leak will occur. We have seen this happen before, both with OpenSSL and other projects.

事前により多くの人に知らせれば、情報がリークする可能性がそれだけ高くなる。OpenSSL でも他のプロジェクトでも、これまでにリークの発生を目にしている。

A huge number of products from an equally large number of organisations use OpenSSL. It's not just secure websites, you're just as likely to find OpenSSL inside your smart TV, car, or fridge.

非常多くの組織、これまた非常に多くの製品が OpenSSL を使っている。OpenSSL はウェブサイトをセキュアにするためだけに使われているわけではなく、スマートTVや車、冷蔵庫などでも使われている。

We strongly believe that the right to advance patches/info should not be based in any way on paid membership to some forum. You can not pay us to get security patches in advance.

パッチやセキュリティ情報を事前に入手する権利は、とあるフォーラムの有料メンバーシップのような形態に基づくべきでない、と我々は強く信じている。我々にお金を払ったからといって、セキュリティパッチは事前に手に入らない。

We can benefit from peer review of the patches and advisory. Keeping security issues private means they can't get the level of testing or scrutiny that they otherwise would.

パッチやアドバイザリのピアレビューから、我々は恩恵をうけることができる。セキュリティ問題をプロジェクト内に留めるということは、公開することで得られるレベルのテストや検証を得られないということである。

It is not acceptable for organisations to use advance notice in marketing as a competitive advantage. For example "if you had bought our product/used our service you would have been protected a week ago".

組織が事前通知をマーケティング上、他社を出し抜くために利用することは受け入れられない。たとえば「我々の製品/サービスを買えば、1週間前に防御できますよ」など

背景事情 (Background) 2/2

There are actually not a large number of serious vulnerabilities in OpenSSL which make it worth spending significant time keeping our own list of vendors we trust, or signing framework agreements, or dealing with changes, and policing the policy. This is a significant amount of effort per issue that is better spent on other things.

実際のところ OpenSSL にそれほど多くの深刻な脆弱性は存在しない。したがって、我々が信頼できるベンダのリストを維持したり、(事前通知のための)フレームワークの契約を結んだり、契約の変更に対応したり、ポリシーを守らせることに膨大な時間を費やす価値はない。

We have previously used third parties to handle notification for us including CPNI, oCERT, or CERT/CC, but none were suitable.

過去に CPNI, oCERT, CERT/CC など第三者機関を使って通知を行ったことがあるが、どれも適切ではなかった。

It's in the best interests of the Internet as a whole to get fixes for OpenSSL security issues out quickly. OpenSSL embargoes should be measured in days and weeks, not months or years.

インターネット全体として考えると、最も肝心なことは、OpenSSLのセキュリティ修正を皆にいち早く提供することである。OpenSSL のエンバーゴーは、月年単位ではなく、日や週の単位で計られるべきものだ。

Many sites affected by OpenSSL issues will be running a version of OpenSSL they got from some vendor (and likely bundled with an operating system). The most effective way for these sites to get protected is to get an updated version from that vendor. Sites who use their own OpenSSL compilations should be able to handle a quick patch and recompile once the issue is public.

OpenSSL の影響を受けるサイトの多くは、なんらかのベンダーから入手したOpenSSLを運用しているだろう(OSにバンドルされている可能性が高い)。これらのサイトを保護する最も効率的な方法は、(管理者が)入手元のベンダーからアップデート版を入手することである。独自にコンパイルしたOpenSSLを使用するサイトであれば、パッチが公開されれば、(自分で)対処できるだろう。

OpenSSL 内でのセキュリティ問題のハンドリング (Internal handling of security issues) 1/3

This leads us to our policy for security issues notified to us or found by our team which are not yet public.

これらの事情を踏まえ、我々に通知された、あるいは我々自身が発見した未公開のセキュリティ問題について、独自の取り扱いポリシーを定めた。

"private" means kept within the OpenSSL development team.

非公開("private")とは OpenSSL 開発チーム内に情報が留まるということを指す。

We will determine the risk of each issue being addressed. We will take into account our experience dealing with past issues, versions affected, common defaults, and use cases. We divide the issues into the following categories:

我々は個々の問題がもたらすリスクを判断する。過去に問題を取り扱った経験や、影響を受けるバージョン、一般的なデフォルトの設定、ユースケースを考慮する。そうして問題を次のカテゴリーに分類する。

OpenSSL 内でのセキュリティ問題のハンドリング (Internal handling of security issues) 2/3

- low severity issues. This includes issues such as those that only affect the openssl command line utility, unlikely configurations, or hard to exploit timing (side channel) attacks. These will in general be fixed immediately in latest development versions, and may be backported to older versions that are still getting updates. We will update the vulnerabilities page and note the issue CVE in the changelog and commit message, but they may not trigger new releases.
- 脅威度低。このカテゴリーには openssl コマンドラインツール、一般的でない設定、脆弱性の悪用が困難なタイミング依存(サイドチャンネル)の攻撃などが含まれる。基本的には最新のバージョンで修正され、アップデートを提供している過去のバージョンにもバックポートする可能性がある。脆弱性のページをアップデートし、changelog やコミットのメッセージでCVEに言及するが、新規バージョンリリースのトリガーにはならないかもしれない。

- moderate severity issues. This includes issues like crashes in client applications, flaws in protocols that are less commonly used (such as DTLS), and local flaws. These will in general be kept private until the next release, and that release will be scheduled so that it can roll up several such flaws at one time.
- 脅威度中。クライアントアプリの異常終了、一般的には使われることのないプロトコル(たとえばDTLS)の欠陥、ローカル(エクスプロイト可能な？)欠陥などが含まれる。このカテゴリーの問題は基本的に次のリリースまで非公開にされる。このカテゴリーの複数の欠陥をまとめて修正するようなスケジュールでパッチが公開される。

- high severity issues. This includes issues affecting common configurations which are also likely to be exploitable. Examples include a server DoS, a significant leak of server memory, and remote code execution. These issues will be kept private and will trigger a new release of all supported versions. We will attempt to keep the time these issues are private to a minimum; our aim would be no longer than a month where this is something under our control, and significantly quicker if there is a significant risk or we are aware the issue is being exploited.
- 脅威度高。一般的な設定に影響を与え、かつ攻撃される可能性が高い問題。サーバのDoS、メモリ内容の漏洩、遠隔からのコード実行など。このカテゴリーの問題は非公開として扱われ、サポート中の全てのバージョンについて修正版を新規リリースする。非公開にする時間は最小限にする努力をする。我々のコントロール下にある問題であれば、目標は1ヶ月以内であり、重大なリスクが存在する場合や攻撃がすでに行われている場合はもっと早くなる。

OpenSSL 内でのセキュリティ問題のハンドリング (Internal handling of security issues) 3/3

During the investigation of issues we may work with individuals and organisations who are not on the development team. We do this because past experience has shown that they can add value to our understanding of the issue and the ability to test patches. In cases where protocols are affected this is the best way to mitigate the risk that a poorly reviewed update causes signficiant breakage, or to detect if issues are being exploited in the wild. We have a strict policy on what these organisations and individuals can do with the information and will review the need on a case by case basis.

問題を調査する間、開発チーム以外の個人や組織と協力して活動することがある。我々がそうする理由は、我々が問題を理解したりパッチを検証することに、彼らが貢献してくれるからである。プロトコルが影響を受ける場合、レビュー不十分なアップデートが大きな問題をもたらすリスクを低減したり、問題が実際に攻撃されているかどうかを検知したりするために、これは最も優れた方法である。これらの個人や組織に対し、情報の取扱いに関して厳格なポリシーを設けており、ケース(問題)ごとに協力を必要とするかを決めている。

事前通知ポリシー (Prenotification policy) 1/2

Where we are planning an update that fixes security issues we will notify the openssl-announce list and update the home page to give our scheduled update release date and time and the severity of issues being fixed by the update. No futher information about the issues will be given. This is to aid organisations that need to ensure they have staff available to handle triaging our announcement and what it means to their organisation.

セキュリティ問題を修正するアップデート(の公開)を計画している場合、openssl-announce リストにその旨を通知するとともに、ウェブページを更新してアップデートのリリース予定日時、問題の脅威度を知らせる。この段階では、問題に関する情報公開はこれらのみとする。この公開は、我々の情報公開をトリアージュできるスタッフを確保し、組織にとって情報が持つ意味を判断できるよう支援するものである。

For updates that include high severity issues we will also prenotify with more details and patches. Our policy is to let the organisations that have a general purpose OS that uses OpenSSL have a few days notice in order to prepare packages for their users and feedback test results.

脅威度高の問題を含むアップデートについては、より詳しい情報とパッチを事前に通知する。我々のポリシーは、OpenSSLを使用する汎用OSを提供する組織が、OS利用者のためにパッケージを準備し、テスト結果を反映させるために必要な数日間の猶予を与えることにある。

事前通知ポリシー (Prenotification policy) 2/2

We use the mailing list described at http://oss-security.openwall.org/wiki/mailing-lists/distros for this. We may also include other organisations that would otherwise qualify for list membership. We may withdraw notifying individual organisations from future prenotifications if they leak issues before they are public or over time do not add value (value can be added by providing feedback, corrections, test results, etc.)

この通知には、http://oss-security.openwall.org/wiki/mailing-lists/distros のメーリングリストを使う。また、このメーリングリストの参加条件に見合うような他の組織を通知先に含めることがある。一般公開前に情報をリークしたり、我々にとって価値がないと判断した組織は(フィードバックをくれたり、修正してくれたり、テスト結果を返してくれるようなところは価値がある)、将来、事前通知先から外すことがある。

Finally, note that not all security issues are notified to us directly; some come from third parties such as companies that pay for vulnerabilities, some come from country CERTs. These intermediaries, or the researchers themselves, may follow a different style of notification. This is within their rights and outside of the control of the OpenSSL team.

最後に、必ずしも全てのセキュリティ問題が我々に直接通知されるわけではない。脆弱性にお金を払う企業のようなサードパーティーの組織から通知されることもあれば、国を代表するCERTから通知されることもあれば、研究者自身から通知されることもあり、彼らの通知スタイルは様々である。どのようなスタイルで通知するかは彼らの権利であり、OpenSSLチームがコントロールできる範囲の外にある。